

THE CORANK OF A RECTANGULAR RANDOM INTEGER MATRIX.

SHAKED KOPLEWITZ

ABSTRACT. We show that under reasonable conditions, a random $n \times (2 + \epsilon)n$ integer matrix is surjective on \mathbb{Z}^n with probability $1 - O(e^{-cn})$. We also conjecture that this should hold for $n \times (1 + \epsilon)n$, and provide a counterexample to show that our “reasonableness” conditions are necessary.

1. INTRODUCTION

In [2], Bourgain, Vu, and Wood show that, given an $n \times n$ random matrix A whose entries take the values $+1, -1$ independently with probability $\frac{1}{2}$, the probability that A is singular is bounded by $(\frac{1}{\sqrt{2}} + o(1))^n$. In particular, this implies that A is injective (as a map $A : \mathbb{Z}^n \rightarrow \mathbb{Z}^n$) with probability $1 - O(e^{-cn})$ for some constant $c > 0$. In this paper, we ask:

Question Let $A : \mathbb{Z}^m \rightarrow \mathbb{Z}^n$ be a random integer matrix (for $m \geq n$). What is the probability that A is surjective?

Our main result is the following:

Theorem 1. *Let A be an ϵ -balanced $n \times (2 + \delta)n$ random matrix with entries $|A_{ij}| = O(2^{n^k})$ for some constant k . Then A is surjective with probability $1 - O(e^{-cn})$ for some constant $c > 0$ as $n \rightarrow \infty$.*

We recall the definition of ϵ -balanced in Section 2.

Some type of independence assumption like ϵ -balancedness is clearly necessary to avoid trivial counterexamples, such as the entries of A all being equal with probability 1. We will also show in Section 4 that the bound on the size is also necessary, for any m , by giving a counterexample when the entries are allowed to be of size up to $e^{3^{nm}}$.

We also show the following holds, as a direct consequence of the results of Wood in [6]:

Theorem 2. *Let A be an ϵ -balanced random $n \times (n + u)$ matrix, with ϵ and $u \geq 1$ constants, then*

$$\limsup_{n \rightarrow \infty} \mathbb{P}(A \text{ is surjective}) \leq \prod_{p \text{ prime}} \prod_{k=1}^{\infty} (1 - p^{-k-u}) = \prod_{k=u+1}^{\infty} \zeta(k)^{-1}$$

If $u = 0$, then $\lim_{n \rightarrow \infty} \mathbb{P}(A \text{ is surjective}) = 0$.

In particular, both results hold for 0-1 Bernoulli random matrices, in which the entries are independently chosen to be 1 with probability q and 0 otherwise, for constant $0 < q < 1$.

We conjecture that under the conditions of Theorem 2, $\lim_{n \rightarrow \infty} \mathbb{P}(A \text{ is surjective}) = \prod_{k=u+1}^{\infty} \zeta(k)^{-1}$. In particular, we guess the following:

Conjecture 1. *Let A be an ϵ -balanced $n \times (1+\delta)n$ random matrix for constant $\epsilon, \delta > 0$, with entries bound by n^k for some constant $k > 0$. Then $\lim_{n \rightarrow \infty} \mathbb{P}(A \text{ is surjective}) = 1$.*

Finally, we ask what we can prove under stronger assumptions. The strongest possible case would be when the entries of the matrix are ‘uniformly distributed’ in \mathbb{Z} . However, there is no uniform distribution over \mathbb{Z} . Our approach to resolving this is to use the Haar measure over the profinite completion $\widehat{\mathbb{Z}}$, which will give us the following theorem:

Theorem 3. *Let $u \geq 0$ be constant, and let $A : \widehat{\mathbb{Z}}^{n+u} \rightarrow \widehat{\mathbb{Z}}^n$ be a random matrix, whose entries are independent identically distributed random variables given by the Haar measure on $\widehat{\mathbb{Z}}$. Then if $u > 0$,*

$$\lim_{n \rightarrow \infty} \mathbb{P}(A \text{ is surjective}) = \prod_{k=u+1}^{\infty} \zeta(k)^{-1}.$$

If $u = 0$, this probability converges to zero.

In particular, Theorem 3, along with the observation that the probability that A is surjective monotonically increases with u , implies the following corollary:

Corollary 4. *Let $u(n)$ be a sequence such that $\lim_{n \rightarrow \infty} u(n) = \infty$, and let $A : \widehat{\mathbb{Z}}^{n+u(n)} \rightarrow \widehat{\mathbb{Z}}^n$ be a random matrix, whose entries are independent identically distributed random variables given by the Haar measure on $\widehat{\mathbb{Z}}$. Then*

$$\lim_{n \rightarrow \infty} \mathbb{P}(A \text{ is surjective}) = 1$$

In particular, this implies that a random $n \times cn$ matrix over $\widehat{\mathbb{Z}}$ with $c > 1$ will be surjective with probability $\rightarrow 1$.

Another natural approach is to take $A = A_{n,m,k}$ to be the matrix whose entries are independent identically distributed random variables uniformly distributed in $-k, \dots, k$, and take $k \rightarrow \infty$. The authors of [5] show that

$$\lim_{k \rightarrow \infty} \mathbb{P}(A_{n,m,k} \text{ is surjective}) = \mathbb{P}(A_{n,m} \text{ is surjective}),$$

where $A_{n,m}$ is a random $n \times m$ matrix over $\widehat{\mathbb{Z}}$.

Acknowledgements. The author is grateful to Sam Payne, Nathan Kaplan, and Van H. Vu for their many helpful suggestions along the way.

This work was partially supported by NSF CAREER DMS-1149054.

2. RESULTS FOR $n \times (n+u)$ MATRICES FOR CONSTANT u

In this section, we prove Theorem 2. We will rely on the following lemma:

Lemma 5. *A matrix $A : \mathbb{Z}^m \rightarrow \mathbb{Z}^n$ is surjective if and only if $A/p : (\mathbb{Z}/p\mathbb{Z})^m \rightarrow (\mathbb{Z}/p\mathbb{Z})^n$ is surjective for every prime p . Here A/p is the matrix over $\mathbb{Z}/p\mathbb{Z}$ given by $(A/p)_{ij} = (A_{ij}) \pmod{p}$.*

Proof. Clearly, if $A : \mathbb{Z}^m \rightarrow \mathbb{Z}^n$ is surjective, so is $A/p : (\mathbb{Z}/p\mathbb{Z})^m \rightarrow (\mathbb{Z}/p\mathbb{Z})^n$ for every p .

Conversely, assume $A/p : (\mathbb{Z}/p\mathbb{Z})^m \rightarrow (\mathbb{Z}/p\mathbb{Z})^n$ is surjective for every p . Then A/p has rank n , and in particular contains an $n \times n$ submatrix $B/p \subseteq A/p$ with nonzero determinant. As $\det(B/p) = \det(B) \pmod{p}$, this implies that $\det(B)$

is nonzero. This implies that the columns of B , considered as vectors over \mathbb{Q} , generate \mathbb{Q}^n as a vector space, and hence $B(\mathbb{Z}^n)$ is a full-rank lattice. But $A(\mathbb{Z}^m)$ is an abelian group containing $B(\mathbb{Z}^n)$, so it must also be a full-rank lattice. In particular, $D = |\mathbb{Z}^n/A\mathbb{Z}^m|$ is finite, and D divides $|\det(B)|$.

But $p \nmid |\det(B)|$, hence $p \nmid D$. As this holds for every prime p , we get $D = 1$, so $\mathbb{Z}^n = A\mathbb{Z}^m$, which completes the proof. \square

In particular, this theorem implies that a square matrix is surjective if it is nonsingular at every prime p . In contrast, a square matrix is injective if it is nonsingular at any prime p .

It is worth noting that the random matrices of [2], whose entries are ± 1 , are never surjective, since $A/2$ is the all-ones matrix.

We now recall the following definition from [6]:

Definition. A random variable y taking values in a ring T is ϵ -balanced if for every maximal ideal \mathfrak{p} of T and every $r \in T/\mathfrak{p}$, we have $\mathbb{P}(y \equiv r \pmod{\mathfrak{p}}) \leq (1 - \epsilon)$. In particular, if T is a field, y is ϵ -balanced if for every $r \in T$, we have $\mathbb{P}(y = r) \leq (1 - \epsilon)$.

A random matrix is ϵ -balanced if its entries are independent and ϵ -balanced.

In particular, a matrix whose entries are independent identically distributed Bernoulli random variables equal to 0 with probability $1 - q > 0$ and 1 otherwise is ϵ -balanced, for $\epsilon = \min(q, 1 - q)$.

For any abelian group G and prime p , define G_p to be its p -Sylow subgroup. If P is a set of primes, define $G_P = \prod_{p \in P} G_p$. We now recall the following theorem of Wood:

Theorem 6 (Corollary 3.4 of [6]). Let $\epsilon > 0$ and let A be an ϵ -balanced $n \times (n + u)$ random matrix. Let G be a finite abelian group and let P be a finite set of primes including all those dividing $|G|$. Then:

$$\lim_{n \rightarrow \infty} \mathbb{P}((\mathbb{Z}^n/(A\mathbb{Z}^{n+u}))_P \simeq G) = \frac{1}{|G|^u |\text{Aut}(G)|} \prod_{p \in P} \prod_{k=1}^{\infty} (1 - p^{-k-u}).$$

Using this, we now prove Theorem 2.

Proof of Theorem 2. Let $A : \mathbb{Z}^{n+u} \rightarrow \mathbb{Z}^n$ be an ϵ -balanced random matrix. By Lemma 5, A is surjective only if A/p is surjective for every prime p . This is equivalent to $(\mathbb{Z}^n/(A\mathbb{Z}^{n+u}))_p$ being the trivial group for every prime p .

Let P be a finite set of primes. Then by Theorem 6 with $G = 1$,

$$\lim_{n \rightarrow \infty} (\mathbb{P}((\mathbb{Z}^n/(A\mathbb{Z}^{n+u}))_p \simeq 1 \text{ for all } p \in P)) = \prod_{p \in P} \prod_{k=1}^{\infty} (1 - p^{-k-u}).$$

But for any finite set P , this is an upper bound on $\limsup \mathbb{P}(A \text{ is surjective})$. Taking P to be increasingly large gives us the theorem. \square

3. SURJECTIVITY OF RANDOM $n \times (2 + \delta)n$ MATRICES

In this section, we prove Theorem 1. First, we recall the following theorem from [3]:

Theorem 7. *Let A be an ϵ -balanced $n \times m$ random matrix over a field \mathbb{F} with $m \geq (1 + \delta)n$ for some constant $\delta > 0$. Then A has full rank with probability at least $1 - e^{-cn}$ for some constant c depending only on ϵ, δ . In particular, c is independent of \mathbb{F} .*

The proof bounds the probability that each row is dependent on the previous rows, similarly to the proof of Lemma 10.

We also cite the following theorem of Maples in [4]:

Theorem 8 (Theorem 1.1 of [4]). *Let A be an ϵ -balanced $n \times n$ random matrix over $\mathbb{Z}/p\mathbb{Z}$. Then we have the estimate*

$$\mathbb{P}(A \text{ is nonsingular}) = \prod_{k=1}^{\infty} (1 - p^{-k}) + O(e^{-cen})$$

where the implied constant and $c > 0$ are absolute.

In particular, we get the following corollary:

Corollary 9. *Let A be an ϵ -balanced $n \times n$ random matrix over \mathbb{Z} . Then*

$$\mathbb{P}(A \text{ is nonsingular}) \geq 1 - e^{-cen}$$

where $c > 0$ is absolute.

Proof. For any prime p , Using Theorem 8 for A/p (changing c if necessary) gives us that

$$\mathbb{P}((A/p) \text{ is nonsingular}) \geq \prod_{k=1}^{\infty} (1 - p^{-k}) - \frac{1}{2}e^{-cen}.$$

Since $\lim_{p \rightarrow \infty} \prod_{k=1}^{\infty} (1 - p^{-k}) = 1$, we can choose p so that $\prod_{k=1}^{\infty} (1 - p^{-k}) \geq 1 - \frac{1}{2}e^{-cen}$, for which we get

$$\mathbb{P}(A \text{ is nonsingular}) \geq \mathbb{P}((A/p) \text{ is nonsingular}) \geq \prod_{k=1}^{\infty} (1 - p^{-k}) - \frac{1}{2}e^{-cen} \geq 1 - e^{-cen}.$$

□

We are now ready to prove Theorem 1.

Proof of Theorem 1. Let A be a random $n \times (2 + \delta)n$ matrix. We split it into two submatrices $A = (B, C)$, where B is $n \times n$ and C is $n \times (1 + \delta)n$. Note that B and C are both ϵ -balanced.

As B is ϵ -balanced, by Corollary 9, it is nonsingular with probability at least $1 - e^{-cn}$, where c depends only on ϵ . Therefore $\det(B) \neq 0$ with probability at least $1 - e^{-cn}$.

We can also bound the size of $|\det(B)|$. Recall that the entries of A , hence in particular the entries B_{ij} of B , are all bounded by $O(2^{n^k})$ for some constant k . Assume that $|B_{ij}| \leq 2^{n^k}$. As the determinant is the sum of $n!$ products of permutations of the B_{ij} , we can bound $|\det(B)| \leq (n!)(2^{n^k})^n \leq 2^{n^{k'}}$ for a sufficiently large constant k' . If $|\det(B)|$ is nonzero, the number of prime divisors of $|\det(B)|$ is bounded by $\log_2(|\det(B)|) \leq n^{k'}$.

Let P denote the set of prime divisors of $|\det(B)|$. By Theorem 7, for every $p \in P$, C/p is surjective over $\mathbb{Z}/p\mathbb{Z}$ with probability $1 - e^{-cn}$. If $\det(B)$ is nonzero, then $|P| \leq n^{k'}$, so the probability that C/p is surjective over every $p \in P$ is at least

$1 - n^{k'} e^{-cn}$. As $\det(B)$ is nonzero with probability at least $1 - e^{-cn}$, the probability that C/p is surjective for every $p \in P$ is at least $1 - (n^{k'} + 1)e^{-cn} \geq 1 - e^{-c'n}$ for some $c' > 0$.

But if this holds, then A is surjective: B/p is surjective over every $p \notin P$, and C/p is surjective over $p \in P$. Hence A/p is surjective over every prime p , so by Lemma 5, A is surjective. \square

4. COUNTEREXAMPLE WITH LARGE ENTRIES

In this section, we show that the bound on the size of the entries given in Theorem 1 is necessary by showing a distribution of the entries with size bounded by $e^{3^{nm}}$, where the probability that a matrix is surjective goes to zero (In fact, the entries will be bounded by $e^{n^2 \log(n)m2^{nm}}$). Note that this depends on m , so taking m to be a large function of n cannot resolve this need for a bound on the size of the entries.

Let P be the set of the first $2^{nm}n$ primes. For each i, j we choose a subset $P'_{i,j} \subseteq P$ independently at random by taking $p \in P'_{i,j}$ independently with probability $\frac{1}{2}$ for every $p \in P$. We let $A_{ij} = \prod_{p \in P'_{i,j}} p$.

A is ϵ -balanced for $\epsilon = \frac{1}{2}$: At a prime $p \in P$, this is obvious, since $\mathbb{P}(A_{ij} \equiv 0 \pmod{p}) = \frac{1}{2}$. for $p \notin P$, this follows by noting that when we choose whether to put the last prime of P in P' , we choose whether or not to change $A_{ij} \pmod{p}$ with probability $\frac{1}{2}$.

To see the bound on the size of A_{ij} , note that A_{ij} is bounded by the product of the first $2^{nm}n$ primes. In general, the product of the first k primes is bounded by $e^{2k \log(k)}$ (see for example [1]). Taking $k = 2^{nm}n$, we see that $|A_{ij}| \leq e^{2^{nm}n \log(2^{nm}n)} \leq e^{n^2 \log(n)m2^{nm}} \leq e^{3^{nm}}$ for all sufficiently large n .

Finally, for every $p \in P$, If all the entries of A are zero mod p , then A is not surjective. For each $p \in P$, this occurs independently with probability 2^{-nm} . As there are $2^{nm}n$ primes in P , the probability of being surjective is at most $(1 - 2^{-nm})^{2^{nm}n} = ((1 - 2^{-nm})^{2^{nm}})^n \leq e^{-n} \rightarrow 0$. This shows that the conclusion of Theorem 1 does not hold in this case.

5. RANDOM MATRICES OVER $\widehat{\mathbb{Z}}$

In this section, we prove Theorem 3.

First, recall that $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$, and that the Haar measure on $\widehat{\mathbb{Z}}$ is the product of the Haar measures on \mathbb{Z}_p . Furthermore, the matrix $A : \widehat{\mathbb{Z}}^m \rightarrow \widehat{\mathbb{Z}}^n$ is the free product of the matrices $A_p : \mathbb{Z}_p^m \rightarrow \mathbb{Z}_p^n$. Where A_p is the $n \times m$ matrix given by taking the \mathbb{Z}_p -part of the coefficients of A . In particular, A is surjective only if A_p is surjective for every p .

When the entries of A are independent random variables in $\widehat{\mathbb{Z}}$, the A_p are all independent random matrices whose values are independent uniformly distributed random variables in \mathbb{Z}_p . Hence

$$\mathbb{P}(A \text{ is surjective}) = \prod_p \mathbb{P}(A_p \text{ is surjective}).$$

The main part of the proof of Theorem 3 is the following lemma:

Lemma 10. *Let A_p be a random $n \times m$ matrix, with $m \geq n$, whose entries are independent and uniformly distributed in \mathbb{Z}_p . Then*

$$\mathbb{P}(A_p \text{ is surjective}) = \prod_{k=m+1-n}^m (1 - p^{-k}).$$

Proof. First, recall that A_p is surjective on \mathbb{Z}_p^n only if A_p/p is surjective on $\mathbb{Z}_p/p\mathbb{Z}_p^n = \mathbb{Z}/p\mathbb{Z}^n$. Hence we can consider A_p/p . Note that its entries are independent and uniformly distributed in $\mathbb{Z}/p\mathbb{Z}$.

As a matrix over a field, A_p/p is surjective only if it has rank n , which happens only if its n rows are independent. We prove by induction that the probability of the first r rows being independent is $\prod_{k=m+1-r}^m (1 - p^{-k})$.

Let u_1, \dots, u_n be the rows of A_p/p . For $r = 1$, u_1 is independent only if it is nonzero. As it has m independent entries, this happens with probability $1 - p^{-m}$. Now assume the claim for r . The first $r+1$ rows, u_1, \dots, u_{r+1} are independent only if u_1, \dots, u_r are independent and u_{r+1} is independent of them. By the assumption, the probability that the first u_1, \dots, u_r rows are independent is $\prod_{k=m+1-r}^m (1 - p^{-k})$. If the first u_1, \dots, u_r rows are independent, there exists some set I of r columns such that $u_1|_I, \dots, u_r|_I$ are independent. Then there are unique coefficients a_1, \dots, a_r such that $u_{r+1}|_I = \sum a_i u_i|_I$, and u_{r+1} is dependent on u_1, \dots, u_r only if $(u_{r+1})_j = \sum a_i (u_i)_j$ for every $j \notin I$. Since $(u_{r+1})_j$ is independent of the rest of the matrix, this happens with probability $\frac{1}{p}$. As there are $m - r$ values for $j \notin I$, this implies that the probability that u_{r+1} is dependent on u_1, \dots, u_r is $p^{-(m-r)}$. Hence overall, the probability that u_1, \dots, u_{r+1} are independent is

$$(1 - p^{-(m-r)}) \prod_{k=m+1-r}^m (1 - p^{-k}) = \prod_{k=m+1-(r+1)}^m (1 - p^{-k}),$$

which completes the proof. \square

We now prove Theorem 3.

Proof of Theorem 3. Let A be a random $n \times (n + u)$ matrix over $\widehat{\mathbb{Z}}$. As we saw,

$$\begin{aligned} \mathbb{P}(A \text{ is surjective}) &= \prod_p \mathbb{P}(A_p \text{ is surjective}) \\ &= \prod_p \prod_{k=u+1}^{n+u} (1 - p^{-k}) \\ &= \prod_{k=u+1}^{n+u} \prod_p (1 - p^{-k}) \\ &= \prod_{k=u+1}^{n+u} \zeta(k)^{-1} \rightarrow \prod_{k=u+1}^{\infty} \zeta(k)^{-1}. \end{aligned}$$

The last two lines hold when $u > 0$. When $u = 0$, $\prod_p (1 - p^{-1}) = 0$, so the product converges to zero. \square

REFERENCES

- [1] J. Barkley Rosser and Lowell Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois Journal of Mathematics*, 6:64–94, 1962.
- [2] Jean Bourgain, Van H Vu, and Philip Matchett Wood. On the singularity probability of discrete random matrices. *Journal of Functional Analysis*, 258(2):559–603, 2010.
- [3] Shaked Koplewitz. p -parts of sandpile groups of random bipartite graphs, in preparation. 2016.
- [4] Kenneth Maples. Singularity of random matrices over finite fields. *arXiv preprint arXiv:1012.2372*, 2010.
- [5] Gérard Maze, Joachim Rosenthal, and Urs Wagner. Natural density of rectangular unimodular integer matrices. *Linear Algebra and its Applications*, 434(5):1319–1324, 2011.
- [6] Melanie Matchett Wood. Random integral matrices and the Cohen-Lenstra heuristics. *arXiv preprint arXiv:1504.04391*, 2015.

MATHEMATICS DEPARTMENT, YALE UNIVERSITY, NEW HAVEN, CT 06511
E-mail address: `shaked.koplewitz@gmail.com`